GOVERNMENT OF INDIA
FINANCE
LOK SABHA

UNSTARRED QUESTION NO:1030
ANSWERED ON:21.07.2017
Online Frauds
Bidhuri Shri Ramesh;Choudhary Shri Ram Tahal;Jaunpuria Shri Sukhbir Singh;Rathwa Shri Ramsinh Patalyabhai;Sawaikar Shri Advocate Narendra Keshav

Will the Minister of FINANCE be pleased to state:

(a) whether the Government has taken cognizance of the increase in the cases of fraudulent embezzlement of money through internet/online/ATM/Debit/Credit Cards;
(b) if so, the details thereof including number of such cases registered and officials found involved in the cases during the last three years and current year, bank and State/Union Territory-wise including Jharkhand;
(c) whether the Government has drawn a cyber crisis management plan to check cyber frauds in the country and if so, the details thereof; and
(d) the steps taken/being taken by the Government to check such frauds and protect customers in this regard?

Answer

MINISTER OF STATE IN THE MINISTRY OF FINANCE

(a) & (b): Information provided by Reserve Bank of India (RBI) on frauds related to ATM / Credit / Debit cards & Net banking during the last three years and current year, state-wise & bank-wise is given in Annex A to E.

(c) & (d): Measures initiated by the RBI to prevent cyber related frauds are given below:

(i) RBI has issued circular on 'Skimming of ATM/Debit/Credit Cards' ,vide No:DBS.Co.FrMC.No.17968/23.10.001/2005-06 dated June 26, 2006, advising banks to take various preventive measures to combat frauds relating to skimming or duplicating of credit cards. The banks, inter alia, were also advised to advise customers not to reveal PIN in response to requests received through e-mail, to periodically verify the transaction history to ensure its correctness and, if any unauthorized transaction was observed it should be immediately reported to the bank and inform the bank if the card is lost or stolen.

(ii) In January 2016, Central Fraud Registry (CFR) has been operationalized at RBI as searchable online central fraud data base for use by the banks in respect of frauds above Rs.1 lakh. The CFR contains critical aspects/ information, including modus operandi in respect of frauds as reported by the banks and select Financial Institutions (FIs). This data base is helpful to the banks not only during credit decisions but also to know about fraud in various areas of banking including cyber frauds, ATM/debit/ credit card and internet banking.

(iii) Caution advices are also issued by RBI as and when necessary for preventing and controlling frauds. Three caution advices have been issued recently in connection with (i) Fraud in Mobile Application (CA No. 4097) (ii) ATMs-Large value cash shortages-Malware attacks (CA No. 4087) and (iii) Fraud-Letter of Comfort -Buyers Credit -Misuse of SWIFT messaging system (CA No.4094).

(iv) RBI has reiterated its instructions vide circular DBS.CO.CFMC.BC.No.6/23.04.001/2016-17 dated September 28, 2016 on funds transfer requirement received through email/fax messages. Banks were advised to strengthen the mechanism put in place by them in this regard and also to adhere to it strictly, including contacting the customer over phone at his registered phone number to ensure genuineness of request of the customer.

(v) In order to focus more attention on IT related matters, Reserve Bank of India has set up a Cyber Security and IT Examination (CSITE) Cell within its Department of Banking Supervision in 2015. RBI has issued a comprehensive circular on Cyber Security Framework in Banks on June 2, 2016 covering best practices pertaining to various aspects of cyber security. The banks are required, among other things, to have a cyber-security policy, cyber crisis management plan, gap assessment vis-Ã -vis the baseline requirements indicated in the circular, monitoring certain risk indicators in the area, report unusual cyber security incidents within 2 to 6 hours, ensure board involvement in the matter and robust vendor risk management. The progress of banks in scaling up their cyber security preparedness is monitored.

(vi) RBI carries out IT Examination of banks separately from the regular financial examination of banks from last year. This report has a special focus on cyber security. The reports have been issued to the banks for remedial action. RBI has also set up Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond to and recover from the incidents. RBI also conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios with the help of Indian Computer Emergency Response Team (CERT-In). RBI also has set up an IT subsidiary, with a focus, among other things, on cyber security within RBI as well as in regulated entities.
*****